AdviSec Ltd

Security Governance

Aims

To be secure Client organisations requires a governance regime which is responsible for setting security objectives, defining 'top-level' policies, organisational structures, and providing the resources required to enable implementation.

Security governance should not be confused with security management: Security management is concerned with making decisions to mitigate risks; governance determines who is authorized to make decisions.

Benefits to Client

An effective governance regime should deliver:

- Increased predictability and reduced uncertainty of business operations
- Protection from the potential for civil and legal liability
- Structure to optimize the allocation of resources
- Assurance of security policy compliance
- Foundation for effective risk management.
- A level of assurance that critical decisions are not based on faulty information
- Accountability for safeguarding information

Process and Execution

Background

Numerous standards and guidance documents are available concerning security governance, including ISO 27001 (International Standard for Information Security Management), Security Policy Framework and the Information Assurance Model (United Kingdom), and even the Official (ISC)2 Guide to the CISSP CBK[1]. It should also be noted that standards governing IT service management (e.g. ITIL and ISO 20000) and 'quality management' (e.g. ISO 9001) are also relevant.

Unfortunately whilst many of these documents encompass 'good practice', they can be generic, and do not take into account the specific requirements of the organisation, or alternatively have been customised to fit a specific requirement.

[1] Certified Information Systems Security Professional

Way forward

Initial

- Step 0: Identify security objectives and constraints
- Step 1: Ascertain the level of compliance with regard to the UK Government's Security Policy Framework and IA Maturity Model
- Step 2: Address any shortcomings with regard to the organisational security structure, including achieving 'buy-in' for key security roles and security bodies. Be clear about the terms of reference, relationship with other organisations / bodies, and security and non-security-related roles.

  Confirm that sufficient resource is available to implement these responsibilities.
- Step 3: Develop a 'top-level' security policy for the organisation(s) and have it 'approved' by the Senior Information Risk Owner.
- Step 4: Establish an information security programme that will serve to develop the remaining 'key' items identified earlier within this paper, e.g. functional and role-based procedures, security architecture, marking scheme for assets , BCP/DR framework and strategy and finally a compliance regime.

Later

- Step 5: Implement the information security programme

Success Criteria

Security governance can be regarded as being 'effective' if the information security programme for the organisation satisfies the following criteria:

- It is an organisational-wide issue
- Leaders are accountable
- It is viewed as an institutional requirement (cost of doing business)
- It is risk-based
- Roles, responsibilities and segregation of duties are defined
- It is addressed and enforced in policy
- Adequate resources are committed
- Staff are aware of their responsibilities and trained
- A development life cycle is required
- It is planned, managed, measureable and measured
- It is reviewed and audited

Outputs

- An organisational structure, including a description of the security roles and responsibilities and security working group / accreditation panel.
- A 'top-level' security policy and functional and role-based procedures.
- A plan for assessing compliance with requirements in the security policy and procedures[2], including requirements for accounting and audit, policy reviews and testing.
- A security documentation set, including a risk assessment and a statement of security controls, for each information system and network containing sensitive information.
- A security marking scheme for information assets that allows the 'severity' of potential Confidentiality, Integrity and non-Availability problems to be stated. Also define a method for assessing the potential 'severity'.
- An organisational-wide security architecture that supports implementation of security controls[3].
- A framework and strategy for business continuity and disaster recovery.

Benefits to Clients

Advisec delivers a professional service based on vendor independence, highly skilled consultants (CLAS, CISSP and ISO 27001 auditors), and underpinned by the knowledge and experience gained through having undertaken several engagements of this type.

Contact us:
Further details, including case studies, presentations and references are available from Nigel Strutt. Please call 07780 526195. Head office; 41, Barry Avenue, Bicester, Oxfordshire. OX26 2DZ. Email: nigel.strutt@advisec.co.uk

[2] Including references to legal and regulatory requirements.

[3] Including references to minimum standards for technical and non-technical controls